505-10-23

MISSION OPERATIONS AND DATA SYSTEMS DIRECTORATE

Earth Observing System Data and Information System (EOSDIS) Security Policy and Guidelines

March 1996

National Aeronautics and Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

Earth Observing System Data and Information System (EOSDIS) Security Policy and Guidelines

March 1996

Prepared Under Contract NAS5-31500
Task Assignment 5509 NFL

Approved by:

Darryl Lakins Date
ESDIS Information Technology Security Official
GSFC, Code 505

Dale Harris Date
Associate Director for Earth Science, Data and Information Project
GSFC, Code 505

This document supersedes *ESDIS Security Program memorandum, dated February 1, 1996*, and all changes thereto.

Goddard Space Flight Center
Greenbelt, Maryland

505-10-23

Preface

Earth Observing System Data and Information System (EOSDIS) Security Policy and Guidelines establishes the policy and responsibilities for ensuring adequate levels of security and integrity for EOSDIS Information Technology processing installations, systems, data, networks and related resources; and constitutes the EOSDIS System Security Policy. This document also provides the guidelines for implementing the policy. This policy applies to all EOSDIS Elements and their Information Technology Resources (ITRs) . An **ITR** refers to any equipment or interconnected system or subsystem(s) of equipment, including networks and their interconnecting hardware, along with the applications used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and information. This also includes the data which resides on the resource.

This document is under configuration control, and the NASA EOSDIS Division is responsible for processing all changes to it. Changes to this document will be issued by document change notice (DCN) or, where applicable, by complete revision. All questions concerning this document should be addressed to:

ESDIS Information Technology Security Official
Code 505
Goddard Space Flight Center
Greenbelt, Maryland 20771

Change Information Page

List of Effective Pages	
Page Number	**Issue**

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
505-10-23	Original	March 1996	

DCN Control Sheet

DCN Number	Date/Time Group (Teletype Only)	Month/ Year	Section(s) Affected	Initials

Section 4. Security Policy Guidelines

Section 5. Responsibilities

Section 1. Introduction

1.1 General

The goal of the EOSDIS security program is to provide cost-effective protection that ensures the integrity, availability, and confidentiality of EOSDIS information technology resources. The objectives are to

- Protect against deliberate or accidental corruption of EOSDIS information technology
- Protect against deliberate or accidental actions that cause EOSDIS information technology resources to be unavailable to users when needed
- Ensure that there is no deliberate or accidental disclosure of NASA sensitive information technology
- Protect against unauthorized access to EOSDOS ITR

1.2 Purpose

This document specifies the policy and responsibilities for ensuring adequate levels of security and integrity for EOSDIS information technology processing installations, systems, data, networks and related resources; and constitutes the EOSDIS System Security Policy.

This document does not replace any security directives, documents, or policies created by the local NASA center or NASA Headquarters, but is an additional requirement for any ITR that has an interface to EOSDIS.

1.3 Scope

This document is applicable to all EOSDIS elements, and to the EOSDIS external elements and users which interface with EOSDIS, except where noted, and applies to interfacing project LANs, administrative LANs, and contractor facilities that support the EOS Project. The EOSDIS elements consist of the EOSDIS Core System (ECS)(which consists of the Distributed Active Archive Centers (DAACs), SMC, DAO, and EOC) the EOS Data and Operations System (EDOS), the EOSDIS Backbone Network (EBnet), the EOS Test System (ETS). The EOSDIS external elements consist of the User Facilities, the Science Computing Facilities (SCFs), the Instrument Support Terminals (ISTs), other interfacing institutions, and the international partners.

1.4 Background

The EOSDIS is a comprehensive data and information system that must perform a wide variety of functions, supporting a diverse national and international user community. EOS data products will be used by a wide spectrum of scientists and the public throughout the extended life of the program and in the decades to follow. This commitment to provide a long-term data base of usable scientific

information to the various user communities distinguishes EOSDIS from current remote sensing data systems. The EOSDIS depends on information technology resources for essential support in accomplishing operational, research, and management objectives.

Therefore, since the EOSDIS information technology resources face identifiable risks of deliberate or accidental misuse, loss, disruption, or destruction, it is essential that steps be taken which are sufficient to ensure that the following occur:

a. networks, systems and data have a high degree of integrity;

b. the potential for abuse or misuse of information technology resources is minimized; and

c. availability of operations is maintained.

1.5 Authority

OMB Circular A-130 and NASA Handbook (NHB) 2410.9A (Chapter 4) provide guidance for determining information technology categories and sensitivity or criticality levels for that information. Once the category and sensitivity or criticality levels have been determined, the handbook establishes a protective-measure guideline that is appropriate when this information is processed by an ITR or transmitted over a communications network. Using this handbook and the referenced documents (Section 1.6), EOSDIS has created this policy and guideline document to provide a more specific set of protective measures and criteria for EOSDIS ITRs.

1.6 Applicable Documents

a. OMB Circular A-130; "Management of Federal Information Resources," February 1996

b. NHB 1600.6, "NASA Communications Security Manual," May 1993

c. "GSFC AIS Security Handbook," March 1994

d. NHB 2410.9A, "NASA Automated Information Security Handbook," June 1993

e. NHB 1620.3C, "NASA Security Handbook," February 1993

f. NHB 2410.7C, "Assuring the Security and Integrity of NASA Automated Information Resources," April 1993

g. "ESDIS Security Program" memorandum, dated February 1, 1996

h. GHB 1600.1A, "GSFC Security Manual," November 30, 1990.

Section 2. Security Policy

2.1 Policy Statement

It is a NASA policy that information technology resources shall be provided a level of security and integrity consistent with the potential harm from their loss, inaccuracy, alteration, unavailability, or misuse. Specifically, actions shall be taken consistent with management determinations of acceptable levels of risk, sufficient to ensure that EOSDIS information technology resources, which include their data, perform the following:

a. incorporate cost-effective management, general, and application controls to provide assurance of the EOSDIS' integrity and accuracy;

b. control interface, communication and data access with cost-effective technical, personnel, administrative, and environmental safeguards;

c. protect from unauthorized access, alteration, disclosure, or misuse of the system resources, and the data processed, stored, or transmitted;

d. maintain the availability of information technology systems and resources for significant scientific missions, programs, and functions;

e. maintain a process that controls changes to any security related and sensitive software, hardware or procedure in the system.

Section 3. Security Policy Elaboration

3.1 Incorporation of Management, General and Application Controls

There are basic elements for an effective security program which need to be employed through a system's life cycle, to protect sensitive, critical, valuable, and important EOSDIS information technology resources (ITRs). These elements according to OMB A-130 and NHB 2410.9A are:

a. Assignment of Sensitivity Levels

b. Security Plan

c. Periodic Risk Assessments

d. Contingency Plans

e. Personnel Screening

f. Security Incident Response

g. Certifications

h. Configuration Management Plan

i. Training.

3.1.1 Assignment of Security Responsibilities

To provide cost-effective protection of the mission-critical, and high technology resources of the EOSDIS system across its diverse computer environments, security responsibilities shall be tiered among a security organization that can be traced to a single focal point in the ESDIS Project Office. The EOSDIS is considered one data processing installation. The set of responsibilities among the EOSDIS security organization is defined in Section 5.0 Responsibilities. See also Figure B-1 in Appendix B for the security organizational chart.

3.1.2 Assignment of Sensitivity Levels

EOSDIS elements shall assign sensitivity levels to their data, interfaces, and systems according to NHB 2410.9A. EOSDIS shall communicate security standards and security requirements through contracts, Interface Control Documents (ICDs), and Memoranda of Understandings (MOUs) to external organizations.

There can be multiple sensitivity levels within EOSDIS elements but the interfaces between EOSDIS elements (e.g., EBnet, EDOS and ECS) will be at the same sensitivity level of the highest sensitivity level of the elements.

All EOSDIS elements shall implement mechanisms (e.g., routing controls, firewalls, gateways, etc.) to allow communications with external interfaces and internal systems with dissimilar sensitivity levels.

3.1.3 Security Plan

Each EOSDIS element shall develop a Security Plan which identifies the specific activities and methods required to implement the EOSDIS Security Policy, as it applies to their systems, data, and interfaces.

All EOSDIS international users shall comply with the controls on systems and networks which process sensitive or mission-critical information, as mentioned in NHB 2410.9A.

3.1.4 Periodic Risk Assessments

Each EOSDIS element shall perform periodic risk assessments for their systems, data, and interfaces. Risk assessments shall be performed :

- Prior to construction or operational use of a new system;
- Whenever there is significant modification to the operational environment or approved configuration baseline of the existing system;
- At periodic intervals, but not to exceed 3 years if no risk assessment has been performed during that time.

3.1.5 Contingency Plans

Each EOSDIS element shall develop and maintain a Contingency Plan which describes the actions to be taken if information technology resources are rendered incapable of performing their intended function by an adverse or disastrous event, which includes the loss or outage of some resource.

3.1.6 Personnel Screening

Personnel who participate in managing, designing, developing, operating, or maintaining computer applications processing sensitive or mission-critical information, or who access automated sensitive or mission-critical information, shall be appropriately screened to a level commensurate with the sensitivity, criticality, or value of the information to be accessed or handled and the risk and magnitude of loss or harm that could be caused by the individual.

3.1.7 Security Incident Response

Each EOSDIS element shall respond to any security incident in their area, as mentioned in NHB 2410.9A. Security incidents must be reported to the ESDIS Project Office. Each EOSDIS element and EOSDIS external element shall develop and document procedures for identifying information technology security incidents and reporting these incidents. Each EOSDIS element shall incorporate these security requirements and procedures in their MOUs with their international partners.

3.1.8 Certifications

All EOSDIS elements shall be certified, by the ITSO or his representative, prior to operational use and shall be recertified at periodic intervals, but not to exceed 3 years. System certification may involve the physical examination and testing of controls and procedures to confirm that they have been implemented.

3.1.9 Configuration Management Plan

All EOSDIS elements shall develop and maintain a Configuration Management (CM) plan which defines the protective measures in place to provide for the integrity, confidentiality, and availability of the EOSDIS ITRs.

Security boundaries shall be established to ensure configuration responsibility. Cost-effective monitoring of interfaces, communications equipment, and computing platforms shall be implemented.

3.1.10 Training

All individuals involved in the management, use, design, development, implementation, maintenance, or operation of the EOSDIS system shall receive ITR security training consistent with the nature of the individual's assigned duties and responsibilities, as well as the sensitivity level of the system.

A continuing Computer Security Awareness Training (CSAT) program will be developed to initially inform and then maintain employee awareness of their security responsibilities, the need for security, and current security practices and information.

3.2 Interface, Communication, and Data Access Controls

The EOSDIS system will consist of multiple ITRS which are networked together, and are also networked to their users. This exposes the EOSDIS system to greater risk, especially when users may be interfacing through public or open networks. The following controls will help lessen this risk:

a. Physical Security

b. Access Controls

c. Identification

d. Authentication

e. Data Encryption

f. Network Security

g. Communications.

3.2.1 Physical Security

All EOSDIS elements shall take protective measures that control access to the logical and physical EOSDIS system. These protective measures, which protect the EOSDIS system from unauthorized access, mistreatment, modification, and destruction or damage, include:

- Controlling Physical Access
- Utilizing Environmental Controls

3.2.2 Access Controls

All EOSDIS elements shall implement access controls commensurate with sensitivity level 2. Access controls shall include procedural and computer security protective measures that facilitate the management of unauthorized access to EOSDIS system resources. All access to EOSDIS billable data and services shall be protected with at least sensitivity level 2 measures.

All users with access to sensitive resources shall be uniquely identified through an individual account. If there is a need for user group accounts, this shall be approved in advance by management. A procedure shall be in place for the creation of new accounts and the removal of accounts no longer needed. All users with access to sensitive resources shall have managed restrictive functional capabilities.

3.2.3 Identification

All users, processes and systems that access EOSDIS systems and information or write to EOSDIS systemsshall identify themselves to EOSDIS. The method of identification shall be dependent upon the resource and network connections of the user when accessing the information. Identification shall not be needed for read only data that is available to the general public and science community. All EOSDIS elements and web interfaces shall provide a warning banner that user's actions may be monitored.

3.2.4 Authentication

All users, processes and systems that write to EOSDIS shall authenticate themselves to EOSDIS. All users, processes and systems that access EOSDIS systems and information shall be authenticated. The method of authentication shall be dependent upon the system resource and network connections of the user when accessing the information. At the very least, passwords shall be used on all EOSDIS ITRs.

Strong authentication (e.g., DCE, Kerberos, MD5, one-time passwords, public key encryption) shall be used when access to EOSDIS is through public networks (e.g., the Internet) or systems that are connected to public networks when accessing the EOSDIS system.

3.2.5 Data Encryption

All sensitive data shall be protected against unauthorized access, alteration, and disclosure. Sensitive data includes financial and proprietary data, spacecraft commands, selected science data, mission critical applications, and any other data that ESDIS management identifies as sensitive.

EOSDIS shall evaluate the need to provide data encryption to sensitive data on a case by case basis. The encryption mechanism selection criteria shall be based on the following:

- Sensitivity level assigned to the data
- Protocol interface requirements of the user.

Agreements between ESDIS management and external organizations shall be established, using Letters of Agreement (LOA), Memoranda of Understanding (MOU), and ICDs when vulnerabilities to either the EOSDIS system or the external system are identified.

3.2.6 Network Security

Each EOSDIS element shall be responsible for the security of their internal networks. All EOSDIS elements shall take protective measures so that information and resources can be shared among users, and still ensure the following:

- Integrity of the transmitted data
- Availability of the network services within an acceptable time period
- Confidentiality of sensitive data.

3.2.7 Communications

All communications links including modems connecting to an EOSDIS element's systems, networks, work stations, or terminals shall be approved by responsible management representatives prior to implementation of the connection. All EOSDIS elements shall provide protected connections to external networks such as Internet.

3.3 Protection of System Resources

All EOSDIS elements shall take protective measures to protect their computer systems against unauthorized access or system use. These protective measures shall include the following:

- Login, LogOff and Timeout Controls
- Utilization of Audit Trails
- Password , Identification and Authentication (I & A) Security
- Database Management System Security
- Physical Protection of All System and Network Elements
- Protection of the computer software and data against destruction and modification.

3.4 Maintaining Availability of EOSDIS

All EOSDIS elements shall take protective measures that are specifically designed to safeguard the EOSDIS system against loss, modification, disclosure, or destruction of its data; and against unavailability of its services. These protective measures include the following:

- Procedures and equipment incorporated with other security measures to protect the various sensitivity levels of data
- Protection and storage of all sensitive data
- Implementation of a CM plan for software utilized on the computer systems
- Backup procedures to recover from disruptions to operations.

3.5 Implementation of Process Control for Security Related Changes

All EOSDIS elements shall develop and maintain a CM process which monitors changes to any security-related or sensitive software, hardware, or procedure for the EOSDIS system. The process shall define the procedures for monitoring these changes in terms of the following:

- Affected security requirements
- Security implications with the change
- Implementation of the change.

Section 4. Security Policy Guidelines

4.1 General

Each EOSDIS Element will provide a level of integrity consistent with management's determination of an acceptable level of risk, sufficient to ensure that the EOSDIS ITRs operate effectively and accurately, and protect data from unauthorized access, alteration, destruction, disclosure, or abuse. The EOSDIS ITRs need to maintain continuous support of EOS missions and programs, while simultaneously incorporating operational and functional controls sufficient to provide assurance of integrity, availability, and confidentiality.

The GSFC AIS Security Handbook provides guidance on how to implement technical, personnel, administrative, and environmental safeguards. All EOSDIS elements and EOSDIS external elements are to utilize this document when performing their self-certification.

The following items are worth discussing since they are applicable to the EOSDIS System:

a. Physical Security

b. System Security Architecture

c. User Identification and Authentication

d. Network Security

e. Security Software

f. Security Monitoring and Auditing

4.2 System Security Architecture

Each EOSDIS element should develop a high-level block diagram of each of their ITRs that depicts the complete hardware configuration of the system and includes all interfaces with external telecommunications and computer systems. This diagram should show all repeaters, servers, bridges, routers, firewalls, and gateway components and describe how these interface devices affect the security of the ITR (e.g., act as a physical switch, require passwords, pass only selected addresses, pass selective protocols).

4.3 Physical Security

The computer equipment should be located in a controlled facility that provides for limited access. The ITR and relevant equipment (e.g., hosts, file servers, network wiring, hubs, routers, gateways, firewalls, terminal servers, etc.) should be secured in rooms with access devices that log and control each individual's entrance to the room.

Since a system console offers a direct access into the system, the system consoles should be located in a secure area. Computer centers with multiple ITRs may want to locate all system consoles separate from the main computer area. Access to the system console should be restricted to the computer operations staff.

Unattended terminals and workstations, especially those logged into a privileged account, are a dangerous security breach and can allow intruders free access to the system with minimal risk of detection. The user community, in unsecured locations, should log off from the system when leaving for a break.

4.4 User Identification and Authentication

One-time or encrypted passwords are preferable for those ITRs with remote access to their networking equipment, hosts or file servers through modems, terminal servers, and TELNET commands.

Systems should refrain from providing banner type information about the system (.e.g., the type of operating system and its version level), or permitting HELP information until after a user has successfully logged into the system, and has been authenticated. All host user accounts and accounts on servers, firewalls, routers, bridges, gateways, terminal servers, and other configurable devices should ensure that user accounts have acceptable passwords or pass phrases that are changed on a regular basis. All default passwords on ITRs should be changed. Formal procedures for administering and controlling the users should be established to keep the authorization records current.

4.5 Network Security

Remote users should be restricted to certain partitioned directories, local files, services and commands. The use of proxy servers is another way to protect commonly utilized services, such as File Transfer Protocol (FTP). In the Client/Server architecture, the LAN operating system will provide the basic system security and audit features. If the operating system does not provide adequate security features, add-on software should be included to satisfy security and audit requirements.

Dial-in interfaces provide widespread exposure of an ITR or network to would-be penetrators. User institutions should minimize this exposure. Break-before-make-type dial-back modems are effective for preventing unauthorized access. Also, modems should have enable passwords, in addition to log-on passwords, for the system. Passwords for dial-in interfaces should be changed periodically**,** especially after personnel or temporary hires have terminated**.** Whenever possible one-time passwords, such as smart cards, or tokens, such as Kerberos, should be implemented. Source routing should be disabled on all routers. TELNET to routers should be disabled and all maintenance and software changes should be initiated from a local console. All configuration and software changes should be maintained under configuration management. Using the same password for more than one router in the same network or network(s) is not recommended because it compromises the other routers when the password on one of the routers is compromised.

4.6 Security Software

The majority of computer systems interfacing with EOSDIS have vendor-supplied or third-party software packages to provide security enhancement(s). Both system and security upgrades should be maintained to ensure the latest defenses against known vulnerabilities.

While each computer manufacturer addresses the security problems and solutions uniquely, there are several common parameters that the self-certification process should address: user Ids, passwords, file, command, and service access, security monitoring and auditing, physical security, and network security.

4.7 Security Monitoring and Auditing

It is recommended that, as a minimum, system auditing include break-in attempts, accesses from detached processes, modifications to user authorization files, and remote accesses.

The audit records should be reviewed bi-weekly, at the minimum.

The network manager should make periodic checks of the network, particularly at the EOSDIS interfaces, to verify proper operation and to detect any unaccountable changes in operations. One or more persons should be assigned to conduct these checks at frequent, random times. A terminal should be designated to monitor network activity, including the EOSDIS interfaces.

4.8 Additional Suggestions

The following procedures are provided as additional ways to enhance the security of the EOSDIS system:

- Identify opportunities to enhance security in the development and maintenance life cycle of user software;
- Search for and identify backdoors, trapdoors, Trojan horses, or similar paths to penetrate the EOSDIS elements, its network, or any of its ITRs, and take steps to nullify them;
- Subscribe to security newsgroups or other publications to keep current on the latest problems and fixes.

Section 5. Responsibilities

5.1 General

The security responsibility will be shared among the ESDIS Project Office, the EOSDIS Element Managers, the ESDIS Information Technology Security Official, the individual EOSDIS Element Security Officials, and the Adhoc EOSDIS Security Working Group (ESWG). The EOSDIS Security Working Group will be comprised of the security officials from both the ESDIS Project and EOSDIS Element levels.

5.2 ESDIS Project Office

Responsibilities of the ESDIS Project Office are divided among the ESDIS Project Management, the ESDIS Project Security Manager, and the EOSDIS Security Working Group.

5.2.1 ESDIS Project Management

The ESDIS Project Management is responsible for:

a. Developing and evaluating the EOSDIS System Security Program;

b. Nominating official representatives associated with each EOSDIS element to Configuration Control Boards, committees, and organizations concerned with the implementation of information technology security and integrity;

c. Coordinating the security documentation sections, as they prepare documentation affecting EOSDIS security, for presentation in boards, committees, or organizations;

d. Ensuring adequate security training of all EOSDIS personnel;

e. Deciding on the disposition of waivers;

f. Ensuring a management official authorizes in writing the use of the EOSDIS system, based on implementation of its security plan and accepting the risk to the system, before operational use or significant modification to the operational environment.

5.2.2 ESDIS Information Technology Security Official (EITSO)

The EITSO is responsible for:

a. Supporting the ESDIS Project management in their security responsibilities;

b. Acting as chairperson of the EOSDIS Security Working Group, which is concerned with maintaining the system security within the ESDIS project;

c. Collecting any security incidents within the Project, and reporting them to appropriate officials;

d. Developing a risk analysis of the EOSDIS system, by assessing the risk analysis from the EOSDIS elements and determining how the vulnerabilities are being managed;

e. Collecting waiver requests within the Project, and reporting them to appropriate officials;

f. Ensuring that the EOSDIS external elements and their interfaces with EOSDIS comply with the security policy in their contracts, Interface Control Documents (ICDs), their Letters of Agreement (LOA), and their Memoranda of Understanding (MOU);

g. Conducting security audits, when necessary, and providing written reports to the ESDIS Project management, and to other appropriate officials;

h. Testing and certifying the security of system interfaces.

5.2.3 EOSDIS Security Working Group

The EOSDIS Security Working Group is responsible for:

a. Reviewing EOSDIS Element Security Plans to ensure compliance with the EOSDIS System Security Policy, and ensuring that no gaps exist in the security coverage across the EOSDIS system;

b. Reviewing reported security incidents and recommending corrective actions (.e.g., installing additional controls, conducting a security audit), if necessary;

c. Evaluating system upgrades and incorporation of new technology to determine if security is affected within their areas;

d. Reviewing waivers and making recommendations;

e. Assisting the EITSO by reviewing the security requirements stated in the external element's contracts, LOAs, and MOUs.

5.3 EOSDIS Elements

The EOSDIS Elements share their responsibilities among the EOSDIS Element Managers, the EOSDIS Element Security Officials, the EOSDIS External Elements, and the EOSDIS International Partners.

5.3.1 EOSDIS Element Managers

The EOSDIS Element Managers are responsible for:

a. Coordinating the development, implementation, and monitoring of each EOSDIS Element System Security Plan. These plans must specify, at a minimum:

1. actions taken to ensure the security, integrity, end user contingency, disaster recovery, and continuity of operations of each installation within the element;

2. actions taken to identify and certify all sensitive applications and data; and

3. actions taken to assure that all acquisitions of information technology resources adequately consider security and integrity issues, and include a schedule for implementation;

b. Participating in the design, development, operation, installation, and maintenance of EOSDIS information technology resources;

c. Promulgating policies and directives that describe and enforce the EOSDIS System Security Policy;

d. Ensuring the interfaces with other EOSDIS Elements are protected by adequate security measures;

e. Implementing NASA or other Government agency certification and accreditation requirements, as appropriate;

f. Reviewing security incidents and violations and written reports sent to the EITSO when a security incident has occurred;

g. Ensuring the adequate training of the Project Element personnel in the areas of security of their ITRs;

h. Assigning a responsible individual in writing to assure that an EOSDIS Element has adequate security. This individual should be knowledgeable in the information and process supported by the Element and in the management, personnel, operational, and technical controls used to protect the Element;

i. Ensuring a management official authorizes in writing the use of an EOSDIS Element based on implementation of its security plan and accepting the risk to the system, before operational use or significant modification to the operational environment.

5.3.2 EOSDIS Element Security Officials

The EOSDIS Element Security Officials are responsible for:

a. Supporting the EOSDIS Element Management in their security responsibilities;

b. Providing or overseeing the day-to-day security operation;

c. Preparing and maintaining a risk assessment process of each EOSDIS data processing installation, including networks, and reporting back to the EITSO and other appropriate officials. The size and scope of the risk analyses should be appropriate to the subject installation. Risk assessments, sufficient to appropriately address the identified risks, shall be conducted and included as a part of the overall ESDIS Project ITR Management Plan;

d. Reviewing all security incidents or violations and providing a written report on all penetration attempts. In addition, provide a verbal report by telephone to the EITSO and to other appropriate officials, on all successful penetrations;

e. Periodically evaluating and recertifying the security safeguards for sensitive applications, and data;

f. Serving as a member of the EOSDIS Security Working Group.

5.3.3 EOSDIS External Elements

The EOSDIS External Elements consist of interfacing NASA and non-NASA institutions. They are responsible for:

a. Developing and implementing a security plan that specifies the security and integrity of any of their ITRs which interface with one or more EOSDIS ITRs;

b. Reporting any security incident or violation to each EOSDIS Element's Security Official for which their affected ITR has an interface;

c. Conducting a periodic risk assessment of each EOSDIS data processing installation, including networks, and reporting back to the EITSO and other appropriate officials. The size and scope of the risk analyses should be appropriate to the subject installation. Risk assessments, sufficient to appropriately address identified risks, shall be conducted and included as a part of the overall ESDIS Project ITR Management Plan;

d. Periodically evaluating and recertifying the security safeguards for sensitive applications, and data.

5.3.4 EOSDIS International Partners

The EOSDIS International Partners are responsible for:

a. Developing and implementing security requirements defined in all MOUs;

b. Reporting any security incident or violation to each EOSDIS Element's Security Official for which their affected ITR has an interface;

c. Periodically evaluating and recertifying the security safeguards for sensitive applications and data

5.4 EOSDIS External Users

The EOSDIS external users are comprised of both the users, whose interfaces with EOSDIS are interactive, and the other external users who are only interested in receiving data from EOSDIS. The interactive users are sustaining engineers, operations and maintenance personnel, scientists, and algorithm maintainers.

5.4.1 Interactive External Users

The Interactive External Users are responsible for:

a. Developing and implementing a security plan that specifies the security and integrity of any of their ITRs which interface with one or more EOSDIS ITRs;

b. Reporting any security incident or violation to each EOSDIS Element's Security Official for which their affected ITR has an interface.

5.4.2 Other External Users

The Other External Users are responsible for:

a. Reporting to the responsible security manager any security incident where data appears corrupted or altered, or if they acquire other than read access with EOSDIS.

Section 6. Waivers

6.1 Waiver Generation

Waiver generation is the user organization's responsibility when an approved security standard cannot be satisfied. Waivers should be submitted for any identified vulnerability as a result of a periodic risk analysis, penetration analysis, self-audit processes, or an official ESDIS Project audit if the vulnerability cannot or will not be corrected within 60 days of its identification.

6.2 Waiver Format

If the self-certification process uncovers a recognizable system vulnerability that will not be corrected within 2 months, a request for waiver must be prepared and submitted to the ESDIS Project Office. The waiver request should describe the vulnerability, proposed solution, impact of the proposed solution on current activities, and expected duration of the waiver.

Appendix A of this document contains a suggested format for the essential elements of a waiver request. The waiver form lists the primary subjects to be addressed (e.g., EOSDIS element or external element, system name, vulnerability description, requested duration of the waiver, and justification). The description of the vulnerability and the wording of the waiver request must provide the essential information necessary to allow for an understanding and an evaluation of the vulnerability by ESDIS Information Technology Security Official. The ITR name and vulnerability description must be sufficiently unique to allow for identity-tracking of the submission. Each waiver request should be on a separate form to assist in the control and processing of requests.

6.3 Waiver Duration

Once a vulnerability is recognized, the ITR's responsible organization should estimate the time and cost to develop a solution. An estimate of the length of time for which the waiver is needed expedites the decision-making process for waiver approval and, establishes a target date for implementation of the fix.

For the convenience of reference, waivers have been divided into three classes:

- Temporary (4 to 6 months)
- Long-term (7 to 36 months)
- Permanent (more than 36 months)

6.4 Submission of Waivers to ESDIS Project Office

All requests for waivers of security vulnerabilities found in an EOSDIS ITR or an ITR interfacing with the EOSDIS system should be forwarded to

ESDIS Information Technology Security Official
Code 505
Goddard Space Flight Center
Greenbelt, Maryland 20771

6.5 Waiver Approvals

The ESDIS Information Technology Security Official, acting as the ESDIS Project Security Manager, will request the ESDIS Security Working Group to evaluate all waiver submissions. If the submission lacks adequate information for a comprehensive evaluation, this group will contact the submitting user organization for additional input, as necessary. The group will make its recommendation for disposition of the waiver, and the ESDIS Project Security Manager will then report to the ESDIS Project Management. Final disposition for the waiver will be given by the ESDIS Project Office. This approval sequence should be completed within 60 days, unless the waiver is of a magnitude such that NASA Headquarters must be consulted.

Appendix A. EOSDIS Security Policy Waiver Request

WR NO.:_____ **DATE RECEIVED.** _____

WAIVER REQUESTED (Specific operational deviation): _____

TYPE (select one): 1:___ 2:____. 3:____ **.EST. RESOLUTION DATE:**_____
(1 = Temporary (4 to 6 months) 2 = Long-Term (7 to 36 months) 3 = Permanent (over 36 months)

(To be filled in by ESDIS Project Office)

DATE:_____

EOSDIS ELEMENT (or EXTERNAL FACILITY):_____

TECHNICAL CONTACT:_____

PHONE NUMBER:_____ **E-MAIL ADDRESS** _____

MAILING ADDRESS: _____

SYSTEM NAME:_____

DESCRIPTION OF VULNERABILITY (use additional sheets, if necessary):

_____

_____

JUSTIFICATION (use additional sheets, if necessary):

_____

_____
Signature of Requester

(To be filled out by ESDIS Project Security Manager and returned to requester)

Assigned Security Analyst:_____

Analyst's comments:_____

_____ Date _____ CONCUR_____ NON-CUR_____

ESDIS Information Technology Security Official

_____ Date _____ APPROVED_____ UNAPPROVED_____

ESDIS Project Management Official

Appendix B. EOSDIS Security Organization

EOSDIS SECURITY ORGANIZATION

The security organization for the ESDIS Project is depicted in Figure B-1.

During the Project Development phase, GSFC Code 500 is responsible, while Code 205 becomes involved as the project goes into an operational phase. The security structure is as follows:

1. The ESDIS Project Manager has the final responsibility for all Project decisions.

2. The ESDIS Information Technical Security Official (ITSO) provides the major inputs on security matters and decisions to the Project Manager.

3. Assisting the ITSO are the Element Managers and their Security Officials.

4. The User Institution's Security Coordinators provide User security information to the Element personnel.

5. As the project becomes operational, the Element Managers and Security Officials also report to Code 205.1.

EOSDIS Security Organization

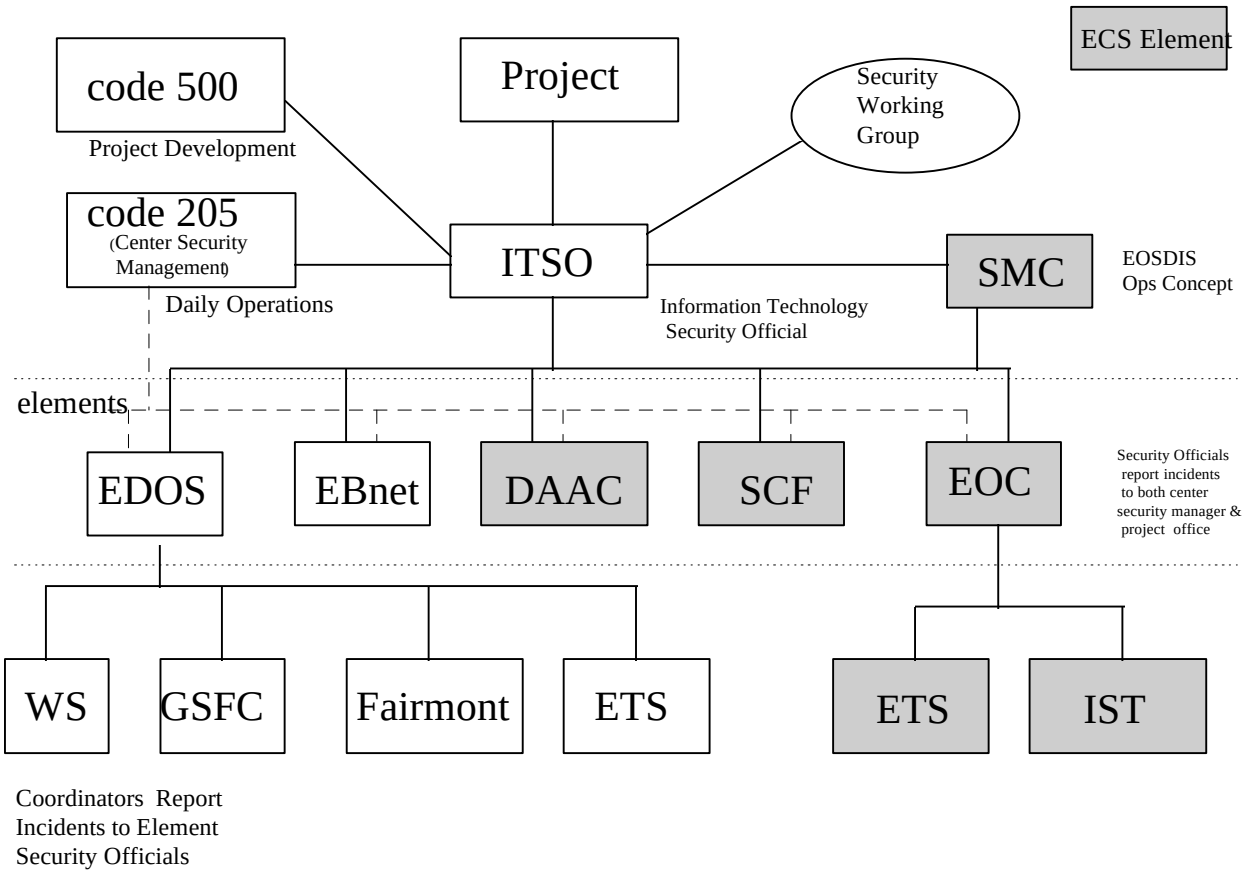

Figure B-1. EOSDIS Security Organization Diagram

Abbreviations and Acronyms

AIS	Automated Information System
CCSDS	Consultative Committee for Space Data Systems
CM	configuration management
CSAT	Computer Security Awareness Training
CSMS	Communications and System Management Segment
DAAC	Distributed Active Archive Center
DCE	Distributed Computing Environment
DCN	document change notice
DES	Data Encryption Standard
EBnet	EOSDIS Backbone (EB) network
ECS	EOSDIS Core System
EITSO	ESDIS Information Technology Security Official
EOS	Earth Observing System
EOSDIS	Earth Observing System Data and Information System
ESDIS	Earth Science Data and Information Support
ESWG	EOSDIS Security Working Group
FDD	Flight Dynamics Division
FOS	Flight Operations Segment
FTP	File Transfer Protocol
GSFC	Goddard Space Flight Center
I & A	Identification and Authentication
ICD	Interface Control Document
ID	identifier
IST	Instrument Support Terminal
ITR	Information Technology Resource
LAN	local area network

LOA	Letter of Agreement
MAN	metropolitan area network
MD5	MD5
MOU	Memorandum of Understanding
NASA	National Aeronautics and Space Administration
NHB	NASA Handbook
NMI	NASA Management Instruction
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
PC	personal computer
QA	quality assurance
SCF	Science Computing Facility
SDPS	Science Data Processing Segment
SMC	System Monitoring and Coordination Center
WAN	wide area network

Glossary

Access	A specific type of interaction between a subject and an object that results in the flow of information from one to the other.
Access Control	The process of limiting access to the resources of a system only to authorized programs, processes, users, or other systems (in a network). Synonymous with controlled access and limited access. Restrictions controlling a subject's access to an object.
Affliated Data Centers	Affiliated data centers (ADCs) and other data centers (ODCs) coordinate data availability with the DAACs and provide selected science data products to the DAACs. EOSDIS elements access the data to satisfy user queries and as correlative data for standard products generated by EOSDIS.
Audit	The process of creating, maintaining, and protecting a chronologica record of system activities that is sufficient to enable reconstructio reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation. a procedure, or event in a transaction from its inception to final results.
Authentication	(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. See PASSWORD as an example. (2) To verify the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized modifications and omission.
Authorization	The granting of access rights to a user, program, or process. This is an administrative capability.
Bridge	A bridge is a device that monitors data on each of the connected LANs and makes decisions about which data packets should be transferred across LANs and which should remain on the LAN whe they were generated. Bridges connect LANs with compatible protocols at the Media Access Control sublayer of the Data Link layer in the OSI protocol model.

Certification	The technical evaluation of a system's security features, made as pa of and in support of the approval or accreditation process, that establishes the extent to which a particular computer system or network's design and implementation meet a set of specified securi requirements.
Communications and System Management Segment	The Communications and System Management Segment (CSMS) provides for the interconnection of users and service providers, transfer of information between the ECS and many EOSDIS components, and status monitoring and coordination of EOSDIS components.
Configuration Management	The management of security features and assurances through contr of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughou the development and operational life of the system.
Data Encryption	The protection of message data passed in a telecommunications system by cryptographic means, from point of origin to point of destination.
Data Encryption Standard	An unclassified algorithm implanted in electronic hardware or firmware devices used for the cryptographic protection of unclassified but sensitive information.
Discretionary Access Control	A means of restricting access to objects based on the identity and need-to-know of the subjects or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing on that permission (perhaps indirectly) to any other subject (unless restrained by mandatory access control).
Distributed Active Archive Centers	The DAACs provide facilities and operations for the production, archive, and distribution of EOS science data products. The DAAC are custodians of EOS mission data and ensure that data are accessible to authorized users. DAACs receive level 0 data from EDOS, the Sensor Data Processing Facility (SDPF), and selected ground stations. DAACs also exchange production planning information with data centers that are part of MTPE but external to the EOS Program, and receive data from these data centers in the form of level 0, ancillary, or processed data sets and the associated metadata.

EOS Data and Operations Center	The EOS Data and Operations Center (EDOS) provides capabilities for handling EOS spacecraft data compatible with the applicable Consultative Committee for Space Data Systems (CCSDS) recommendations. EDOS performs forward-link processing of command data, captures science and housekeeping data from the spacecraft and instruments, processes telemetry to generate level 0 products, and maintains a backup archive of level 0 products.
EOS Test System	The EOS Test System (ETS) provides an early source of CCSDS formatted data during EOSDIS development and a variety of simulation and test support functions to verify EOSDIS elements, interfaces, and capabilities throughout the system life cycle. The ET can simulate EOSDIS systems, other EGS elements, and EOS spacecraft.
EOSDIS Backbone Network	The EOSDIS Backbone Network (EBnet) provides communication circuits and facilities between and among various EGS elements, to support mission operations and to transport mission data between EOSDIS elements.
EOSDIS Core System	The EOSDIS Core System (ECS) provides the services and functionality to command and control the EOS spacecraft and instruments, process data from the EOS instruments, and manage a distribute EOS data products and other selected data sets. The ECS consists of three segments defined to support three major operation areas: flight operations, science data processing, and communications and system management.
EOSDIS Elements	An EOSDIS facility that generates, archives, and distributes EOS Standard Data Products, and related information, for the duration o the EOS mission. An EOS Element is managed by an institution such as a NASA field center or a university, under terms of agreement with the EOSDIS Project.
EOSDIS External Elements	An EOSDIS facility that generates, archives, and distributes EOS Standard Data Products, and related information, for the duration o the EOS mission. An EOS Element is managed by an institution such as a NASA field center or a university, under terms of agreement with the EOSDIS Project.

Firewall	A collection of components used to block or filter transmission of certain classes of traffic. There are three types of firewalls: packet filtering, circuit gateways, and application gateways.
Flight Operations Segment	The Flight Operations Segment (FOS) manages and controls the EOS spacecraft and instruments. The FOS is responsible for missio planning, scheduling, control, monitoring, and analysis in support mission operations for U.S. EOS spacecraft and instruments. The FOS consists of two elements, the EOC and the Instrument Support Terminal (IST).
Gateway	A hardware device that provides a communication path between tw LANs using different LAN types and protocols. Gateways may perform protocol conversion for all seven layers of the Open Syste Interconnection (OSI) model and may be application-specific.
Identification	The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names, and special login mechanism.
Information Technology Resource	Any equipment or interconnected system or subsystem(s) of equipment, including networks and their interconnecting hardware, along with the applications used in the automatic acquisition, storag manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and information. Th also includes the data which resides on the resource.
Local Area Network	The connection of ITRs within a local area. LANs use a serialized bus with a cable length of up to several kilometers. LANs are local networks with relatively short ranges and are commonly used withi a single building or floor.
Metropolitan Area Network	A computer network that connects several ITRs within a metropoli area. MANs are extensions of shared-access LANs (i.e., extended t the size of a city and its suburbs) and are designed to take advantag of the high speeds possible with fiber optics.

Object	A passive entity that contains or receives information. Access to an object potentially implies access to the information it constrains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printer and network nodes.
Password	A private character string used to authenticate an identity of a user prior to accessing a system or network.
Process	A program in execution. A process is completely characterized by single, current execution point (represented by the machine state) a address space.
Repeaters	Repeaters connect two similar LANs at the OSI physical layer or cable. Both media must be the same (i.e., a repeater can connect tw Ethernets or two Token Rings, but not an Ethernet to a Token Ring Repeaters simply repeat signals received on one LAN to the other.
Risk Assessment	An identification of a specific computer facility's assets, the threats these assets, and the computer facility's vulnerability to those threa Risk assessment is a management tool that provides a systematic approach for: • Determining the relative value and sensitivity of computer installation assets • Assessing vulnerabilities • Assessing loss expectancy or perceived risk exposure levels • Documenting management decisions.
Routers	Routers connect LANs with common protocols at the network laye and above. Because routers connect at the network layer, they are protocol-sensitive and thus can link two TCP/IP, DECnet, or XNS-based LANs, but not their combinations.
Science Computing Facility	SCFs are used by EOS investigators to develop algorithms and models for the generation of standard and special products, assess data and data product quality, and conduct science research. The investigators access instrument data at the DAACs and receive science data products, and provide high-order data products, nstrument calibration data, product quality analysis results, science data processing software, and science research results to the DAAC

Science Data Processing Segment	The Science Data Processing Segment (SDPS) provides for the generation and maintenance of EOS science data products for distribution to users. It provides the science community with the infrastructure to access EOS science data and with products resultir from research activities that utilize these data. The SDPS is a distributed system located at the DAACs and the SCFs.
Security Architecture	The subset of computer architecture dealing with the security of the computer or network system.
Security Incident	Any circumstance or event which has harmed or has the potential t harm the system in the form of destruction, disclosure, modificatio of data, and/or denial of service.
Security Level	The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of information. The currently accepted method of determining the security level fo NASA is NHB 2410.9. This handbook defines the various security or criticality levels and lists the generic protection requirements for each level.
Security Policy	The set of laws, rules, and practices that regulate how an ITR manages, protects, and distributes sensitive information.
Sensitivity Levels	Four NASA hierarchical groupings, labeled 0 through 3, used to he determine which computer security controls are needed. See NHB 2410.9A, "NASA Automated Information Security Handbook."
System Monitoring and Coordination Center	The SMC provides the capabilities necessary to manage ECS resources, at the ECS site level and for EOSDIS system-wide resources.
Subject	An active entity (generally in the form of a person, process, or devi that causes information to flow among objects or changes the syste state. Technically, a process and domain pair.
User	Person or process accessing an ITR either by direct connection (i.e. via terminals) or by indirect connection (i.e., via preparation of inp data or receipt of output data that is not reviewed for content or classification by a responsible individual).
Vulnerability	A weakness in system security procedures, system design, implementation, internal controls,etc., that could be exploited to violate system security policy.

Waiver	A request for relief from meeting a security standard or practice un a satisfactory solution can be implemented to correct a known vulnerability.
Wide Area Network	A network or interconnection of ITRs over a large geographic area such as between cities.

Distribution List

Organization	Name of Recipient	Copies
GSFC/170	Price, Mr.	1
GSFC/300	Bauman, Mr.	1
GSFC/421	Scolese, Mr.	1
GSFC/422	Donahoe, Mr.	1
GSFC/424	Peterson, Ms.	1
GSFC/430	Obenschain, Mr.	1
GSFC/500	Fuchs, Mr.	1
GSFC/510	Perkins, Ms.	1
GSFC/530	Liebrecht, Mr.	1
GSFC/540	Turner, Mr.	1
GSFC/205	Middleton,Mr.	1
GSFC/541	Torain, Mr.	1
GSFC/505	Harris, Mr.	1
GSFC/505	Lakins, Mr.	1
GSFC/541	Tomardy, Mr.	1
GSFC/541	Hill, Mr.	1
		14
GSFC/505	All ESDIS personnel	